(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 624 644 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.02.2006 Bulletin 2006/06

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(21) Application number: **05106967.2**

(22) Date of filing: **28.07.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **02.08.2004 US 909633**

(71) Applicant: **NOVELL, INC.**
Provo, Utah 84606 (US)

(72) Inventors:
- **Carter, Stephen R.**
  Spanish Fork, UT 84660 (US)
- **Burch, Lloyd Leon**
  Payson, UT 84651 (US)
- **Ebrahimi, Hashem Mohammad**
  Salt Lake City, UT 84108 (US)
- **McClain, Carolyn B.**
  Springville, UT 84663 (US)

(74) Representative: **Curley, Donnacha John et al**
Hanna, Moore & Curley,
11 Mespil Road
Dublin 4 (IE)

(54) Privileged network routing

(57) Techniques are provided for establishing privileged paths for data packets over a network. A data packet is received (210) with a header; the header includes a route selector (502). The route selector assists in resolving a privileged path (240) for the data packet. The data packet is injected (250) into the network over the resolved privileged path.

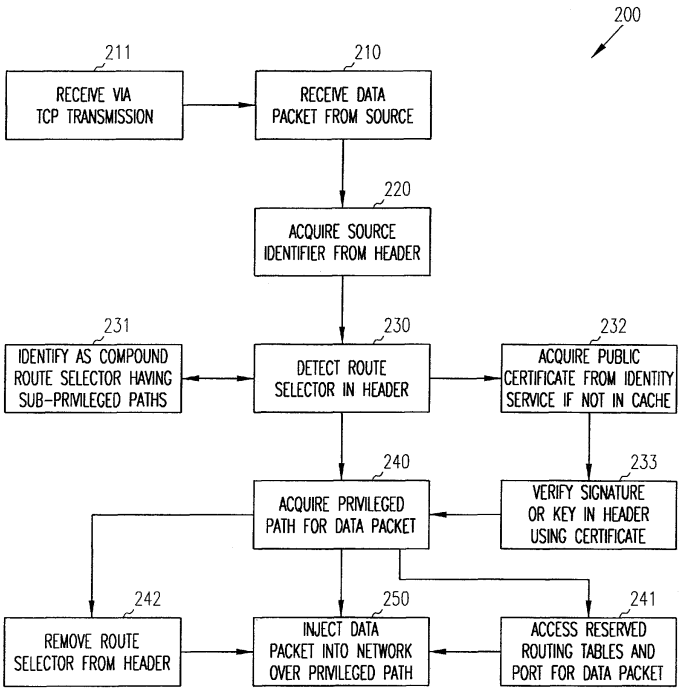

FIG. 2

EP 1 624 644 A2

Description

Field of the Invention

[0001] The invention relates generally to networking and more specifically to techniques for establishing privileged network routing of data.

Background of the Invention

[0002] Networks are rapidly becoming overloaded and taxed with traffic from governments, organizations, and private individuals. In particular, the Internet is increasingly being used to conduct business, acquire information, and for leisure. Moreover, there have been recent governmental efforts made to ensure all participants within the United States have affordable access to high speed connectivity to the Internet. However, if every participant were to have a high speed connection to the Internet, then websites will become even more overtaxed and not be capable of supporting the increased speed with which transactions are received and processed.

[0003] As a result, organizations and Internet Service Providers (ISPs) have begun selling high-end services, such as Virtual Private Networks (VPNs) to customers. A VPN ensures a dedicated port for traffic over a network for participants of the VPN, where traffic over that port is custom encrypted based on the participants to that VPN. The encryption provides an added enticement to customers, because it adds security aspects to transactions over the VPN. However, because ports are finite resources only so many VPNs can be realistically available. Moreover, the VPN encryption requires applications which must be supported on the client devices of the participants.

[0004] With the introduction of VPN and similar services, the Internet is rapidly becoming segmented into fast and secure networks for those that can afford it and legacy (slower) and insecure networks for those that cannot afford it. Furthermore, if VPNs are excessively deployed, the Internet may begin to logically resemble a finite collection of dedicated networks, where fees are required to traverse across each separate dedicated network. This may actually hinder the true purpose of the Internet, which was to provide pervasive connectivity to services and information in an uninhibited manner. If tolls are required to proceed at various points of the Internet, then usage of the Internet will be severely inhibited.

[0005] Another problem, which has only strengthened the movement towards VPN solutions, is the increased threat of malicious interference with Internet traffic. That is, a network transaction may include sensitive information which can be maliciously grabbed or may be tainted with a virus that may damage resources that process the transaction. In fact, this problem has become so pervasive that governments, organizations, and individuals have invested heavily in devices and software to detect and prevent such behaviour.

[0006] Even without VPNs, the Internet is rapidly becoming congested and there is a need for new private and privileged networks existing as sub-networks within the Internet. Such privileged networks would provide enhanced network service to organizations for effectively continuing to do business over the Internet by offering privileged routes over the Internet, which are reserved for selective subscribers. Therefore, there is a need for improved network transactions which offer alternatives to traditional VPN and related technologies and which provide privilege networks.

Summary of the Invention

[0007] The present invention provides methods, systems and data structures for privileged computer network routing in accordance with claims which follow. In various embodiments of the invention, techniques are presented for establishing privileged paths for data packets over a network. A data packet having a header is received. The header includes a detected route selector. The route selector identifies or resolves a privileged path for the data packet over a network. The data packet is injected into the network over the identified or resolved privileged path.

[0008] More specifically, and in an embodiment, a method for injecting a data packet into a network over a privileged path is described. A data packet is received from a source and a route selector is detected in a header of the data packet. In response to the route selector, a privileged path is acquired and the data packet is injected into the network over the privileged path.

Brief Description of the Drawings

[0009]

FIG. 1 is a diagram of an example architecture view of a privileged path injection system, according to an example embodiment of the invention.

FIG. 2 is a flowchart of a method for injecting a data packet into a network over a privileged path, according to an example embodiment of the invention.

FIG. 3 is a flowchart of another method for injecting a data packet into a network over a privileged path, according to an example embodiment of the invention.

FIG. 4 is a diagram of a privileged routing system, according to an example embodiment of the invention.

FIG. 5 is a diagram of data packet header for injecting a data packet into a network over a privileged path, according to an example embodiment of the invention.

Detailed Description of the Invention

[0010] In various embodiments of the invention, the term "path" is used. A path includes a plurality of network nodes. A node may be any network resource or processing device, such as a client, a server, a proxy, a mass storage device, etc. Nodes are connected via a network and interfaced with one another using a variety of protocols or interfaces, some interfaces are associated with hardware and some are associated with software. The interfaces may be layered, meaning that higher- level interfaces are used by applications or users interfacing on the nodes and are converted into a variety of other lower-level interfaces for purposes of performing a network transaction.

[0011] Further, each node may be interfaced to a variety of other processing devices and other LANs. The processing devices execute applications and a number of related applications cooperate to form systems. Any particular code can be designated as a source node, an intermediate node, or a destination within the network. A source node initiates a network transaction from one of its applications or systems executing on one of its processing devices. An intermediate node assists in relaying or forwarding a source node's transaction through the network to a destination node. Any particular network transaction may be handled by a multitude of intermediate nodes before it reaches its destination node. A destination node has the processing device, application, system, or storage medium that is the object of the source node's transaction.

[0012] The designation of a node within a network as a source, intermediate, or destination node is relative. This means that one node may receive a designation for one transaction and a different designation for another transaction. Typically, a node that initiates a network transaction will drive designations for the other participating nodes that will handle the transaction. During a transaction over a network, the paths that the transaction may take can be viewed as a sub-network for that transaction. A path is a subset of nodes, connections, and/or resources that define how the transaction may move from the source node through zero or more intermediate nodes to the destination node.

[0013] A "privileged path" is a path that is processed by at least one node of the network in a special manner. That is, a node may designate and use reserved or special routing tables and/or ports to provide a higher priority to data packets associated with a privileged path. In this manner, a data packet associated with a privileged path receives priority processing throughput through the node that recognizes it. It should also be noted that not all nodes that process a data packet associated with a privileged path will receive or even be aware of the privileged path association to the data packet.

[0014] A network transaction includes a source node (hereinafter "source") that desires to transmit data over a network to a destination node (hereinafter "destination"). That data for the transaction is broken into a series of one or more data chunks called data packets for purposes of efficiently transmitting the entire block of data through a path of the network from the source to the destination. This process of breaking and sending the data as data packets for a given transaction is handled by conventional network protocol, such as, but not limited to Transmission Control Protocol (TCP), and others.

[0015] In various embodiments of the invention, an identity service is used. The identity service provides a trusted technique for authenticating resources participating in network transactions. The identity service may also provide identity information and authenticating mechanisms to resources, such that one resource can become trusted and authenticated to another resource. In this sense, the identity service is a trusted intermediary and facilitator to the resources of the network.

[0016] The identity service may also provide a variety of other services. Examples of an identity service can be found in our European Patent Applications Nos. 04 106 396.7 ("Techniques for Dynamically Establishing and Managing Authentication and Trust Relationships"), 05 100 336.6 ("Techniques for Establishing and Managing a Distributed Credential Store"), and 05 100 358.0 ("Techniques for Dynamically Establishing and Managing Trust Relationships".

[0017] In one embodiment, the techniques presented herein are incorporated into network arrangements, services, and products, such as proxy services, routers, gateways, and the like. These techniques inject data packets associated with a network transaction into a network over a privileged path in the manners described herein and below.

[0018] FIG. 1 is an architectural diagram of one privileged path injection system along with an example data packet flow through the injection system, according to an example embodiment of the invention. The injection system is implemented in a machine accessible and readable medium over a network within various resources of that network. A variety of network protocols, software, hardware, are also used during operation of the injection system The injection system selectively identifies data packets and injects them into a network over privileged paths.

[0019] The architectural diagram 100 shows a variety of components that participate processing a data packet, The data packet moves through the injection system for a given network transaction. These components include an injection service 101, a source 102, a secure network 103, m identity service 104, an insecure network 105, one or more intermediate nodes 106 and 107, and a destination 108.

[0020] The source 102 and the injection service 101 are within a secure and potentially trusted relationship within a secure network 103. FIG. 1 shows the source 102 straddling the secure network 103 because in some instances the source 102 may enter the secure network 103 from a different insecure network (not shown in FIG.

1). That is, the source 102 may originate within the secure network 103 or may originate from a different network, in which case the source 102 authenticates itself and becomes a participant within the secure network 103.

[0021] For example, consider a source 102 that is a laptop that has travelled outside the secure network 103. Such a source 102 may use an insecure network, such as the Internet, to contact a firewall of the secure network 103, authenticate itself, and thereby become a temporary participant within the secure network 103. In an alternative example, the laptop may be docked within a LAN associated with the secure network and may become a participant to the secure network by simply logging into the secure network.

[0022] The injection service 101 is a proxy service, a router, a gateway, a switch, a hub, a bridge, etc. The source 102 may or may not be aware of the presence of the injection service 101. Additionally, the source 102 may itself be a proxy service, application, router, gateway, etc. Thus, the source 102 does not have to be the device used by a sender of a network transaction. That is, the sender may use an application or service on one device to initiate a network transaction, where that network transaction is sent to or intercepted by the source 102. The source 102 may also be aware or unaware of the injection service 101, such as when the source 102 directly processes the transaction to the injection service 101 or alternatively when the injection service 101 intercepts network transactions being processed by the source 102 to a desired destination 108.

[0023] When the source 102 is ready to transmit one or more data packets associated with the transaction to the injection service 101 via link A, the source 102 may perform a variety of operations. In some cases, as described above this may entail the source authenticating to the secure network 103. In one embodiment, this authentication occurs via an identity service 104, such as the identity service described above.

[0024] Once authenticated the source 102 acquires one or more route selectors for the transaction. A route selector is a piece of data (may be a data structure) that identifies a privileged path (C1, C2, and C3) over the network 105 for the transaction. Additionally, a route selector may include nested sub-route selectors associated with sub-privileged paths. Furthermore, a route selector may be a string of route selectors each associated with a different or complementary privileged path over the network 105 from the source 102 to the destination 108.

[0025] In one embodiment, the source 102 acquires one or more route selectors from the identity service 104 after authentication to the secure network 103. That is, the identity service 104 manages distribution of route selectors based on identities of senders, sources 102, injection services 101, networks 105, and/or destinations 108. In another embodiment, an external service (not shown in FIG. 1) manages distribution of route selectors, such that the source 102 acquires information on how to authenticate to that external service via the identity service 104, and once authenticated requests the route selectors from the external service. In still other embodiments, the source 102 may itself have an embedded route selector management service that provides the route selectors to the source 102. In yet other embodiments, the injection service 101 may manage and distribute sets, lists, or individual route selectors to the source 102 for the source 102 to independently manage or use on a per-request basis.

[0026] Once the source 102 has one or more route selectors for the transaction that it is processing on behalf of a sender, each data packet associated with the transaction is associated with the route selector(s). Association can be 30 achieved in a variety of manners via metadata associated with a data payload of the data packet. One technique is to modify a conventional TCP header (metadata) for a data packet by adding the route selector data to that header's options segment. By placing this information in the options segment normal and legacy TCP/IP operation for network protocols will not be impacted. Moreover, the only entity that is aware of the modified options segment and that will be looking for it is the injection service 101.

[0027] Optionally, the metadata may also include an identity for the source 102 or sender of the network transaction, a digital signature of the source 102 or sender, and/or other configurable keys or chains of keys established by policies. In one embodiment, the metadata also includes the identity for the source 102 and a digital signature of the source 102, where the digital signature includes the route selector data and a 32-bit TCP sequence number associated with the data packet (by including the 32-bit TCP sequence number, man-in-the-middle attacks become essentially worthless). This additional metadata associated with the data packet provides security to the network transaction.

[0028] Once the metadata is configured by the source 102, it is associated with the data packet (e.g., as a data packet header) and sent to the injection service 101 over link A. In one embodiment, the packet is sent from the source 102 to the injection service 101 via traditional TCP/IP network communication. The injection service 101 strips the metadata and detects the presence of one or more route selectors and optionally security information (ids, signatures, and/or keys).

[0029] If the injection service 101 detects security information or by policy requires security information for the transaction, then the injection service 101 contacts the identity service 104 over link B for purposes of acquiring keys and/or satisfying itself that the transaction is legitimate. Accordingly, in one embodiment, the injection service 101 acquires a public certificate for the source 102 from the identity service 104. In one embodiment, the public certificate is cached by the injection service 101, such that it is available for subsequent privileged path processing associated with the source 102. Thus, in some cases, the injection service 101 does not have to contact the identity service 104, since the public

certificate is pre-existing in cache. The public certificate permits the injection service 101 to validate a signature or other keys embedded in the metadata of the data packet sent from the source 102. If the security information is not verified then the injection service 101 can deny the transaction or ignore the request for a privileged path for the transaction and process the data packet with conventional routing tables and ports accessible to typical network transactions within the injection service 101. Optionally, the injection service 101 may also log and/or report any invalid attempts to acquire a privileged path for a network transaction.

[0030] If the security information is verified, when present and used, or not present when not used, then the injection service 101 strips the route selector(s) from the received data packet and acquires the privileged path(s) associated with the route selector(s) and sends the data packet and its privileged path(s) to reserved routing tables and ports accessible to the device processing the injection service 101. In one embodiment, a selective first portion of the privileged path is also stripped out by the injection service 101. The first portion is the link and node information associated with moving the data packet from the injection service 101 to a first intermediate node. This portion of the privileged path is no longer necessary, since the next receiving intermediate node of the data packet and the privileged path only needs its next portion of the privileged path. In this manner, stripping the route selectors and selective first portions of the privileged path ensures that the data packet includes only a minimal amount of needed metadata to process through the network. The data packet receives priority service from the injection service 101 and is processed more rapidly than conventional data packets would be handled by the injection service 101.

[0031] In one embodiment, for purposes of decreasing the size of the metadata associated with the data packet and improving processing throughput through the network 105, the injection service may also strip the route selector(s) and/or any included security information from the metadata before forwarding the data packet and its privileged path(s) to the reserved routing tables and/or port.

[0032] Once the data packet is sent to the reserved routing tables and/or port, it is injected into the network 105 from the injection service 101 over the privileged path (C1, C2, and C3) to the destination 108. The identifier for the intermediate node 107 is included in the privileged path and sent as metadata with the injected data packet. The identifier for intermediate node 106 is not needed and may be optionally stripped from the privileged path (C2 and C3) because the injection service 101 processes the data packet to the first portion of the privileged path (C1). Moreover, the intermediate nodes 106 and 107 do not need to be aware of the concept of the privileged path or the processing that took place with the source 102, the injection service 101, and the identity service 104 within the originating secure network 103.

[0033] In some embodiments, the injection service 101 may decide when a data packet that is validated and has a route selector is to receive a privileged path and determine dynamically which privilege path to provide the data packet. For example, the injection service 101 may use policies to decide that at certain times of the day or on certain calendar days a privileged path is provided to data packets.

[0034] Alternatively, configurable events or conditions, such as processing load may dictate whether a privileged path is even needed, even when one is requested. For example, a data packet may request via its metadata a privileged path, but the injection service 101 may detect that the normal routing tables and ports are grossly underutilized in comparison to the reserved routing tables and/or port associated with privileged path processing. In these situations, the injection service 101 by policies may elect not to provide a privileged path to the requesting data packet.

[0035] In another mode of operation, the source 102 or sender may be external to the secure network 103 and become part of the secure network via authentication through assistance of the identity service 104. In some cases, the connection used by such a source 102 or sender to authenticate to the secure network 103 can be a VPN.

[0036] It should also be noted, that the network 105 need not be an insecure Wide Area Network (WAN) such as the Internet in all embodiments of the invention. That is, in some embodiments, the network 105 is another secure network associated with an organization, such that the privileged path becomes a sub-network or overlay within the secure network 105.

[0037] Furthermore, in some embodiments where security information is implemented, the keys used to validate a data packet having a route selector need not be associated with signatures of the sources 102 or senders and need not be associated with encryption. That is, additional keys independent of source 102 or sender identity can be used. Keys may also be independent of encryption. Moreover, as previously stated, multiple keys can be used and chained together via policies.

[0038] FIG. 2 is a flowchart of one method 200 for injecting a data packet into a network over a privileged path. The method 200 (hereinafter "injection service") is implemented in a machine-accessible and readable medium and is enable d to process over networks using conventional network connections, resources, arrangements, and protocols. In one embodiment, the injection service is the injection service 101 of FIG. 1 and the descriptions that follow more fully detail its processing and embodiments.

[0039] At 210, the injection service receives a data packet from a source associated with a desired network transaction of the source, where the source desires the data packet to be sent over a network to destination using a privileged path. In one embodiment, at 211, this packet is received from the source via a TCP/IP transmission.

In other embodiments, the packet is received via any conventional or custom-developed protocol having modified metadata (header data) designed to achieve the teachings presented herein.

[0040] When the injection service receives the data packet, it acquires, at 220, a source identifier from the data packet header. This source identifier uniquely identifies the sender of the data packet and is included in traditional network protocols. At 230, the injection service detects a route selector that is also present in the header. The route selector is a novel data structure or string that is unobtrusively placed in the header by the source. By unobtrusive it is meant that the route selector is in a reserved or unused area of the data packet header that will not cause legacy network protocols to fail or recognize it during normal transmissions. For example, in one embodiment, the route selector data may be placed in the options segment of a TCP header.

[0041] It should also be noted that the route selector identifies or assist the injection service in resolving a privileged path for the received data packet. Moreover, a single header may include a string or multiple route selectors associated with multiple of sub-privileged paths. That is, route selector data be nested within a header and thus identified as a compound route selector, at 231.

[0042] In some embodiments, where trusted and secure transmissions are desired, the header may also include security information, such as signatures and keys. The decryption and validation of these signatures and keys may not be known a priori to the injection service. Thus, at 232, the injection service uses the source identifier of the source to contact an identity service for purposes of acquiring a public certificate of the source or sender. However, if, at 232, the public certificate of the source was previously cached, then the injection service can acquire the public certificate from cache and does not have to contact the identity service. Moreover, in some embodiments, the injection service does cache the public certificate of the source after it is initially acquired from the identity service. At 233, the public certificate permits the injection service to verify signatures of the source or sender and/or keys included with the security information present in the header. Again, if security information is being used and if it is not validated the data packet's request for a privileged path may be ignored and processed over a non-privileged path, or alternatively the network transaction associated with the requesting data packet may be discarded and not processed at all.

[0043] At 240, a privileged path is acquired for the detected and identified route selectors of the header, Acquisition can occur in a variety of manners. For example, the injection service may independently determine the proper privileged path based on policies, conditions, or events. Alternatively, there may be a mapping between the route selector and the privileged path that is resolved by reserved routing tables accessible to the injection service. Still further, the injection service may maintain or access a data store that maps route selectors, sources, and/or destinations to predefined privileged paths.

[0044] Once a privileged path is acquired, at 240, the injection service forwards or relays the data packet to a set of reserved routing tables and/or port(s), at 241, that process privileged paths for data packets. These routing tables and/or port(s) may be managed and set aside by the injection service permanently or when certain conditions warrant that they be set aside. Thus, the injection service can free up any reserved routing tables and/or port(s) when there are no privileged paths being processed and other routing tables and/or port(s) are loaded down on the device processing the injection service.

[0045] In some embodiments, for purposes of efficiency of processing the data packet, at 242, the injection service may strip the route selector(s) and any security information from the header before sending the data packet to the reserved tables and/or port or before placing the data packet on the network over the privileged path. The injection service may also strip a selective first portion of the privileged path, since it is the injection service that forwards the data packet over the link and node information associated with the first portion of the privileged path. This ensures that the data packet will not have additional data that increases the size of the packet which may impact its throughput through the network. Moreover, any intermediate nodes along the privileged path do not need to be aware of the privileged path or its processing which is achieved by the injection service. In this manner, legacy routers, proxies, hubs, bridges, gateways, and the like are not impacted and process normally once receiving the data packet and its privileged path from the injection service.

[0046] At 250, the injection service injects the data packet and its header into the network over the privileged path. That is, metadata or the header of the data packet includes the intermediate nodes of the privileged path which are needed to transmit, relay, or forward the data packet over the network to the destination.

[0047] In one embodiment, the privileged path may also include alternative privileged sub-paths, such that should any intermediate node of the original privileged path fail or one of its connections, the last intermediate node having the data packet can select and alternative sub-privileged path from the existing metadata of the data packet.

[0048] FIG. 3 is a flowchart of another method 300 for injecting a data packet into a network over a privileged path, according to an example embodiment of the invention. The method 300 (again referred to as injection service, herein and below) is implemented in a machine -readable and accessible medium and is accessible over networks using conventional network arrangements, resources, and protocols. The injection service presents alternative embodiments and perspectives to the injection service described above with respect to method 200 of FIG. 2.

[0049] At 310, the injection service receives a data packet having metadata and a data payload. The payload

is data which is associated with a network transaction originating from a source or sender and directed to a destination over a network. In one embodiment, the metadata is part of the data packet's header that is included with the data payload. In another embodiment, the metadata augments a data packet's header with additional information not included in the header. In one specific example embodiment, the metadata is a TCP header having conventional TCP fields for TCP header information, where the teachings presented herein are implemented in the options segment of that TCP header, so as to not impact legacy TCP processing associated with the data packet.

[0050] At 311, the data packet is received from a source or sender either from a source originating within a secure network having the injection service or from a source or sender that authenticates remotely to the secure network and becomes a temporary participant in the secure network. At 312, the route selector and signature and/or key security information are stripped from the metadata for purposes of subsequent processing defined herein and below. Moreover, a selective first portion of the privileged path is stripped from path, since this portion is processed by the injection service.

[0051] At 320, the identity of the source sending the data packet is verified In one embodiment, verification may occur in the following manner. At 321, a signature of key of the source is verified with a public certificate of the source. That public certificate may be permanently housed within the environment (cache or storage) of the injection service or may be configured or manually supplied to the injection service. Alternatively, at 322, the injection service dynamically acquires the public certificate of the source by contacting and interacting with an identity service, in the manners described herein and above.

[0052] If the identity of the source is not verified, then, at 323, the injection service may deny processing of the data packet altogether or may elect or be configured based on policy to inject the data packet into the network over a non- privileged path associated with normal non-privileged path processing.

[0053] If the identity of the source is verified, then, in one embodiment, at 324, the route selector and any security information included within the metadata are stripped from the metadata of the data packet. This improves processing throughput through the network once the data packet is injected into the network over the privileged path by reducing the data packet size.

[0054] Once the identity of the source is verified, at 320, the data packet, at 330 can be injected into the network over the privileged path. In some embodiments, the route selector directly identifies the privileged path. In other embodiments, the injection service dynamically resolves the privileged path to be associated with the data packet.

[0055] FIG. 4 is a diagram of a privileged routing system 400, according to an example embodiment of the invention. The privileged routing system 400 is implemented in a machine-readable and accessible medium and is enabled to pr ocess within network arrangements, with network resources, and with network protocols. In one embodiment, among other things, the privileged routing system 400 implements the methods 200 and 300 of FIGs. 2 and 3.

[0056] The privileged routing system 400 includes a route selector data structure 401 and an injection service 402. Optionally, the privileged routing system 400 also includes an identity service 403, such as the one described herein and above. Moreover, in some embodiments, the privileged routing system 400 includes an administrative interface 404.

[0057] The route selector data structure 401 is data that assists in resolving or determining a privileged path for a data packet. The route selector data structure 401 is included in metadata of a data packet. In one embodiment, the route selector data structure 401 is included in the options segment of legacy TCP data 30 packet headers. The route selector data structure 401 may include one or more route selectors. That is, the route selector data structure 401 may have nested route selectors associated with nested, sub, and/or alternative privileged paths for a given data packet. The route selector data structure 401 is carried around with a data payload of a data packet. In this manner, a data packet includes the metadata having the route selector data structure 401 and a data payload.

[0058] In some embodiments, the metadata also includes security information, such as a key, chain of keys, and/or signatures. This security information may be encrypted with the identity of a source or sender that initially constructs the data packet. The security information permits the injection service 402 to verify the authenticity of the data packet having the route selector data structure 401.

[0059] The injection service 402 verifies the identity of the source or sender, acquires a privileged path for the data payload of the data packet based on the route selector data structure 401, and injects the data packet into a network over the privileged path. To perform verification, the injection service 402 may enlist the help of an identity service 403. Additionally, the injection service 402 may cache some or all of the security information or any public certificates or keys acquired from the identity service 403.

[0060] The identity service 403 performs a variety of useful features that may leverage various embodiments of the invention. Examples of specific identity services 403 were described above. More specifically, the identity service 403 may hold credentialing information for participants within network configurations that permit these participants to dynamically acquire techniques and identity information needed to interact with one another. In one embodiment, the identity service 403 also provides for the management and distribution of route se lector data structures 401 to sources requesting the same for

network transactions. In more embodiments, the identity service 403 provides the injection service 402 with decryption keys, or public certificates which can be used by the injection service 402 to verify any security information included in the metadata and associated with the source and the route selector data structure 401.

[0061] The injection service 402 may also be interfaced to an administrative interface 404. This permits the injection service 402 to be configured with policies, conditions, events, privileged paths, etc. The administrative interface 404 may also be used to define the route selector data structure 401 to the injection service 402.

[0062] The injection service 402 may maintain mappings between instances of the route selector data structures 401 and privileged paths. Alternatively, the injection service 403 may permit route selector data structures 401 that are representative of groups of available privileged paths. In these situations, the route selector data structure 401 may even be supplied within the metadata of the data packet as a wildcard value. Moreover, the injection service 402 may override based on policy specific requests for privileged paths that are identified by the route selector data structure 401. Overrides may be may be based on policy, configurable conditions, and/or configurable events.

[0063] In one embodiment, the injection service 402 may interact in a novel manner with the identity service 403 for purposes of informing a source or sender that keys are being changed for certain route selector data structures 401 or privileged paths. These changes are sent up to the identity service 403 and then sent down from the identity service 403 to the source or sender.

[0064] Once the injection service 402 verifies the identity of the source or sender, satisfies itself as to the authenticity of the route selector data structure, and resolves a privileged path, the injection service 402 injects the data packet into the network over the privileged path. In some cases, the route selector data structure 401 and any security information included within the metadata are stripped prior to injecting the data packet into the network over the privileged path.

[0065] FIG. 5 is a diagram of one data packet header 500 for injecting a data packet into a network over a privileged path, according to an example embodiment of the invention. The data packet header 500 is implemented in a machine-accessible or readable medium and is carried around at least initially with data packets involved in network transactions. In one embodiment, the data packet header represents the metadata described above with reference to FIGS. 1-4. In this sense the data packet header 500 facilitates the processing of the methods 100, 200, and the system 400.

[0066] The data packet header 500 includes a source identifier 501, a route selector data structure 502, and a signature 503. In some embodiments, the data packet header 500 also includes other traditional information carried with network packets, such as, but not limited to, sequence numbers for the packets, destination identifiers, acknowledgement numbers, port numbers, checksum values, offset values, and the like. In one embodiment, the route selector 502 and signature 503 are embedded within the options segment of a legacy TCP data packet header.

[0067] The source identifier 501 identifies a source or sender of a data packet. Again, the data packet includes a header or metadata having the data packet header 500, other information, and a data payload (the data the source wants to direct to a destination). The route selector 502, as described herein and above, is data or a data structure that permits an injection service to resolve a privileged path for the data packet to traverse over a network to its destination.

[0068] The signature 503 may be an encrypted signature of the source which may be encrypted with a chain of keys, or a key independent of the source that is provided by the injection service via an identity service and then through the identity service to the source for use and placement within the data packet header 500. In some cases, the signature 503 is also independent of any particular encryption.

[0069] In one embodiment, the signature 503 is generated by the source using the source identifier 501, the route selector 502, and a 32-bit sequence number for the data packet provided by TCP/IP network protocols. In another embodiment, the signature 503 is encrypted by the source with a private key of the source and a public key of the injection service. In this latter embodiment, the injection service may hold the public key or certificate of the source or may dynamically acquire it as needed from the identity service.

[0070] The route selector 502 can include nested instances of other route selectors 502. These sub-route selectors 502 are associated with one or more additional sub-privileged or alternative paths for the data payload of the data packet within the network.

[0071] A source constructs the data packet header 500 and an injection service consumes the data packet header 500. The injection service verifies the source and route selector 502, resolves a privileged path for the network path, optionally removes the route selector 502 and the signature 503, and injects the data packet into the network over the resolved privileged path.

[0072] Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art will appreciate that any arrangement calculated to achieve the same purpose can be substituted for the specific embodiments shown. This disclosure is intended to cover all adaptations or variations of various embodiments of the invention. It is to be understood that the above description has been made in an illustrative fashion only. Combinations of the above embodiments, and other embodiments not specifically described herein will be apparent to one of ordinary skill in the art upon reviewing the above description.

Claims

1. A method for injecting a data packet into a network over a privileged path (C1, C2, C3), comprising:

   receiving (210) a data packet;
   detecting (230) a router selector associated with the data packet;
   acquiring (240) a privileged path associated with the route selector; and
   injecting (250) the data packet into a network over the privileged path.

2. The method of claim 1 further comprising, acquiring (232) a public certificate of a source for the data packet from an identification service before injecting (250) the data packet into the network.

3. The method of claim 2 further comprising, verifying a signature or key included in a header of the data packet in response to the public certificate before injecting (250) the data packet into the network.

4. The method of claim 1 further comprising, removing (242) the router selector from a header of the data packet before injecting (250) the data packet into the network.

5. The method of claim 1, wherein receiving (210) further includes receiving the data packet having a header from the source via a Transmission Control Protocol (TCP), and wherein an options segment of the header includes the route selector.

6. The method of claim 1, wherein detecting (230) further includes identifying (231) the route selector as a compound route associated with the privileged path which has a plurality of sub-privileged paths embedded therein or identifying the route selector as being associated with the privileged path and one or more alternative privileged paths.

7. The method of claim 1, wherein injecting (250) further includes, accessing (241) a port and routing tables reserved for the privileged path and other privileged paths.

8. A method for injecting a data packet over a privileged network, comprising:

   receiving (310) a data packet having metadata that includes a route selector for a privileged path (C1,C2,C3);
   verifying (320) an identity of a source that sends the route selector, and
   injecting the data packet into a network over the privileged path, if the identity of the source is verified.

9. The method of claim 8, wherein receiving (310) further includes:

   stripping (312) a source identifier from the metadata; and
   stripping (312) a signature or key from the metadata.

10. The method of claim 8, wherein verifying (320) further includes verifying (321) a signature or a key with a public certificate of the source.

11. The method of claim 10 further comprising at least one of:

    dynamically contacting (322) an identity service to acquire the public certificate of the source; and
    acquiring a previously retained public certificate of the source from at least one of cache and storage.

12. The method of claim 8 further comprising, stripping (324) the route selector from the metadata before injecting the data packet into the network.

13. The method of claim 8, wherein receiving (310) further includes receiving the data packet and metadata from a source within a secure network (103), wherein the source is a trusted entity to the processing of the method.

14. The method of claim 13, wherein receiving (310) further includes receiving (311) the data packet and metadata from a source that previously authenticated itself to the secure network (103) via an insecure network (105) thereby entering the secure network.

15. A privileged routing system (100,400), comprising:

    a route selector (502) data structure (401) associated with metadata of a data packet that originates from a source (102); and
    an injection service (101,104,402) that verifies an identity of the source, acquires a privileged path assigned to the route selector, and injects the data packet into a network over the privileged path if the source is verified.

16. The privileged routing system of claim 15, wherein the injection service (402) is at least one of a router, a gateway, and a proxy processing within a secure network.

17. The privileged routing system of claim 15, wherein the metadata is a portion of a Transmission Control Protocol (TCP) header.

18. The privileged routing system of claim 15 further comprising, an administrative interface (404) for defining the route selector (502) and the privileged path to the injection service.

19. The privileged routing system of claim 15 further comprising, an identity service (403) accessible to the injection service (402), wherein the injection service communicates with the identity service to acquire identity information (501) for the source, and wherein an identity for the source is also included within the metadata.

20. The privileged routing system of claim 19, wherein the metadata also includes a key or signature (503) of the source encrypted with the identity information (501) of the source and the route selector (502), and wherein the injection service (402) verifies the source by acquiring a decryption key or public certificate for the source from the identity service (403), the decryption key or public certificate used to verify the key or signature.

21. The privileged routing system of claim 15, wherein the injection service (402) resolves the privileged path based on configurable events or conditions.

22. The privileged routing system of clam 15, wherein the injection service (402) changes a key to be used within the metadata for the data packet and transmits the key to an identity service (403), the identity service communicates the key to the source and the source resends the data packet to the injection service with a revised version of the metadata having the key.

23. The privileged routing system of claim 15, wherein the metadata also includes at least one of a signature (503) of the source and a key for the privileged path.

24. A data packet header (500) residing in a machine readable medium, comprising:

a source identifier (501);
a route selector (502); and
a signature (503) for the source identifier and the route selector, wherein the signature validates a source associated with the source identifier, and the route selector resolves a privileged path for a data payload associated with the data packet header over a network.

25. The data packet header of claim 24, wherein the data packet header is a Transmission Control Protoc ol (TCP) header having a modified options segment that includes the route selector (502) and signature (503).

26. The data packet header of claim 25, wherein the signature (503) includes an encrypted version of source identifier, the route selector, and a 32 bit sequence number for the data payload provided with the TCP header.

27. The data packet header of claim 24, wherein the signature (503) is encrypted with a private key of the source and a public key of an injection service.

28. The data packet header of claim 27, wherein the signature (503) is decrypted with a public certificate of the source.

29. The data packet header of claim 24, wherein the route selector (502) includes nested sub-route selectors associated with one or more additional sub-privileged paths for the data payload.

30. The data packet header of claim 24 further comprising, a chain of sub-keys that are chained by a policy associated with the source.

31. A computer program which when executing on a computer or computer network performs the method of any one of claims 1 to 7, or 8 to 14.

32. The computer program of claim 31, when stored on a machine readable medium.

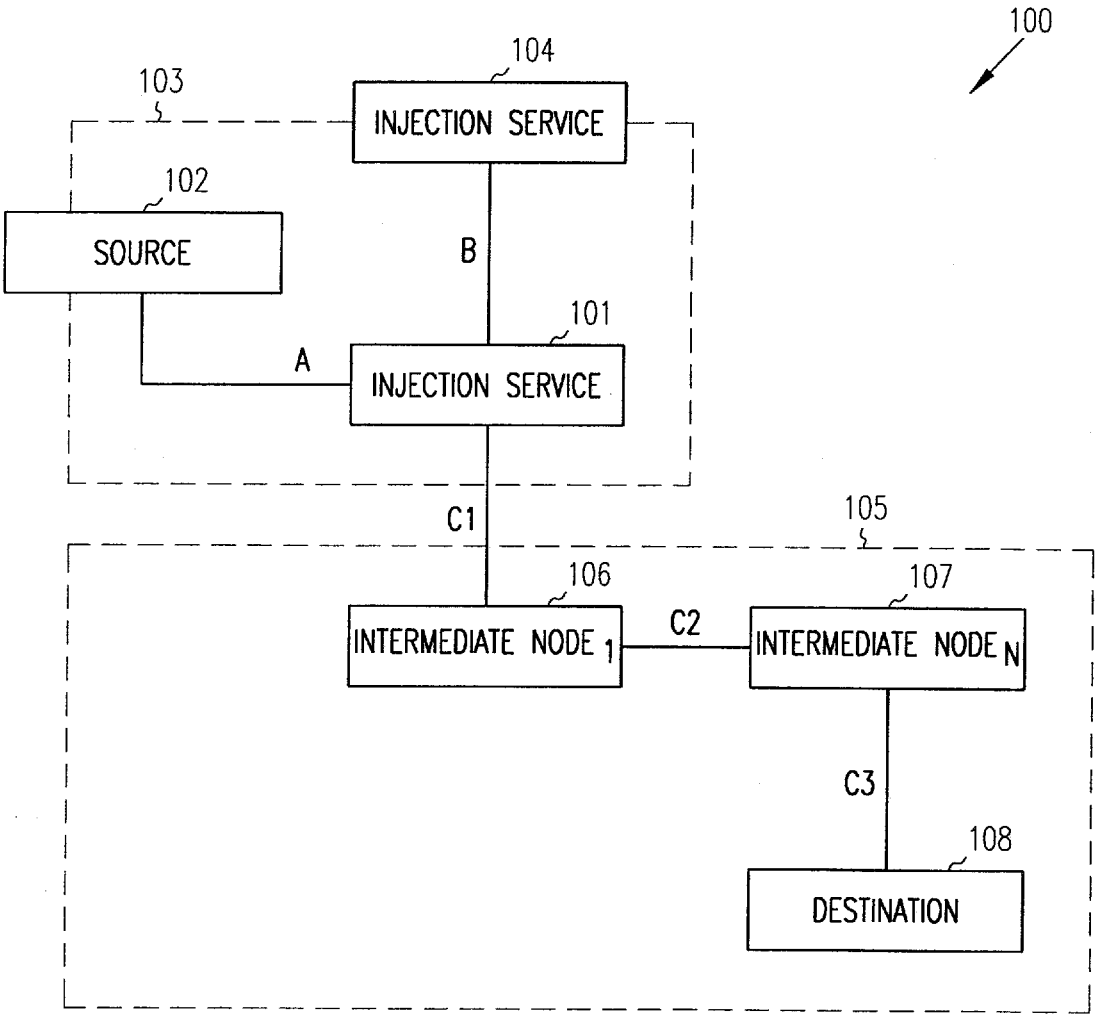
100
104
103
INJECTION SERVICE
102
SOURCE
B
101
A
INJECTION SERVICE
C1
105
106
107
INTERMEDIATE NODE 1
C2
INTERMEDIATE NODE N
C3
108
DESTINATION

FIG. 1

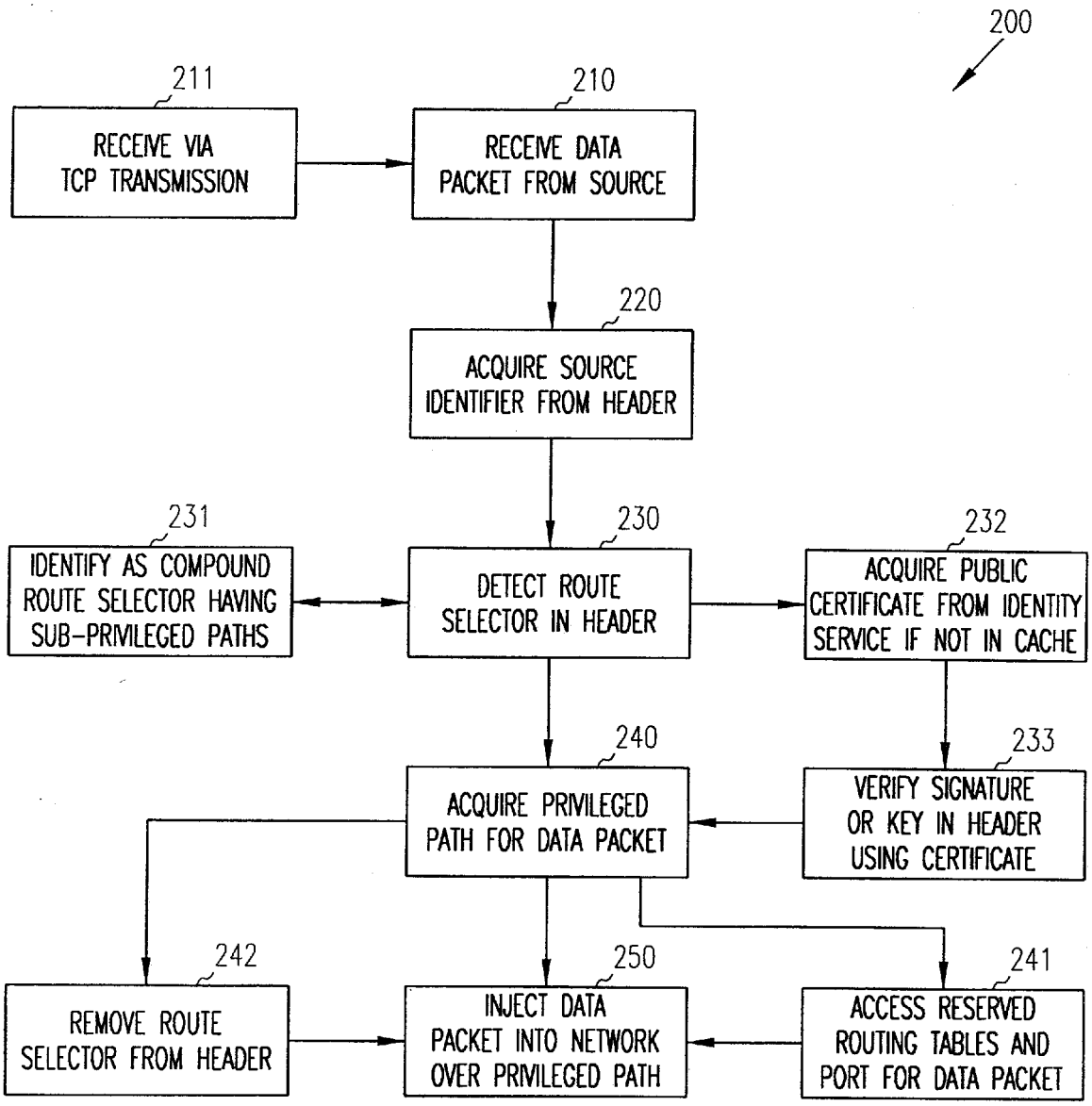
200
211
RECEIVE VIA TCP TRANSMISSION
210
RECEIVE DATA PACKET FROM SOURCE
220
ACQUIRE SOURCE IDENTIFIER FROM HEADER
231
IDENTIFY AS COMPOUND ROUTE SELECTOR HAVING SUB-PRIVILEGED PATHS
230
DETECT ROUTE SELECTOR IN HEADER
232
ACQUIRE PUBLIC CERTIFICATE FROM IDENTITY SERVICE IF NOT IN CACHE
240
ACQUIRE PRIVILEGED PATH FOR DATA PACKET
233
VERIFY SIGNATURE OR KEY IN HEADER USING CERTIFICATE
242
REMOVE ROUTE SELECTOR FROM HEADER
250
INJECT DATA PACKET INTO NETWORK OVER PRIVILEGED PATH
241
ACCESS RESERVED ROUTING TABLES AND PORT FOR DATA PACKET

FIG. 2

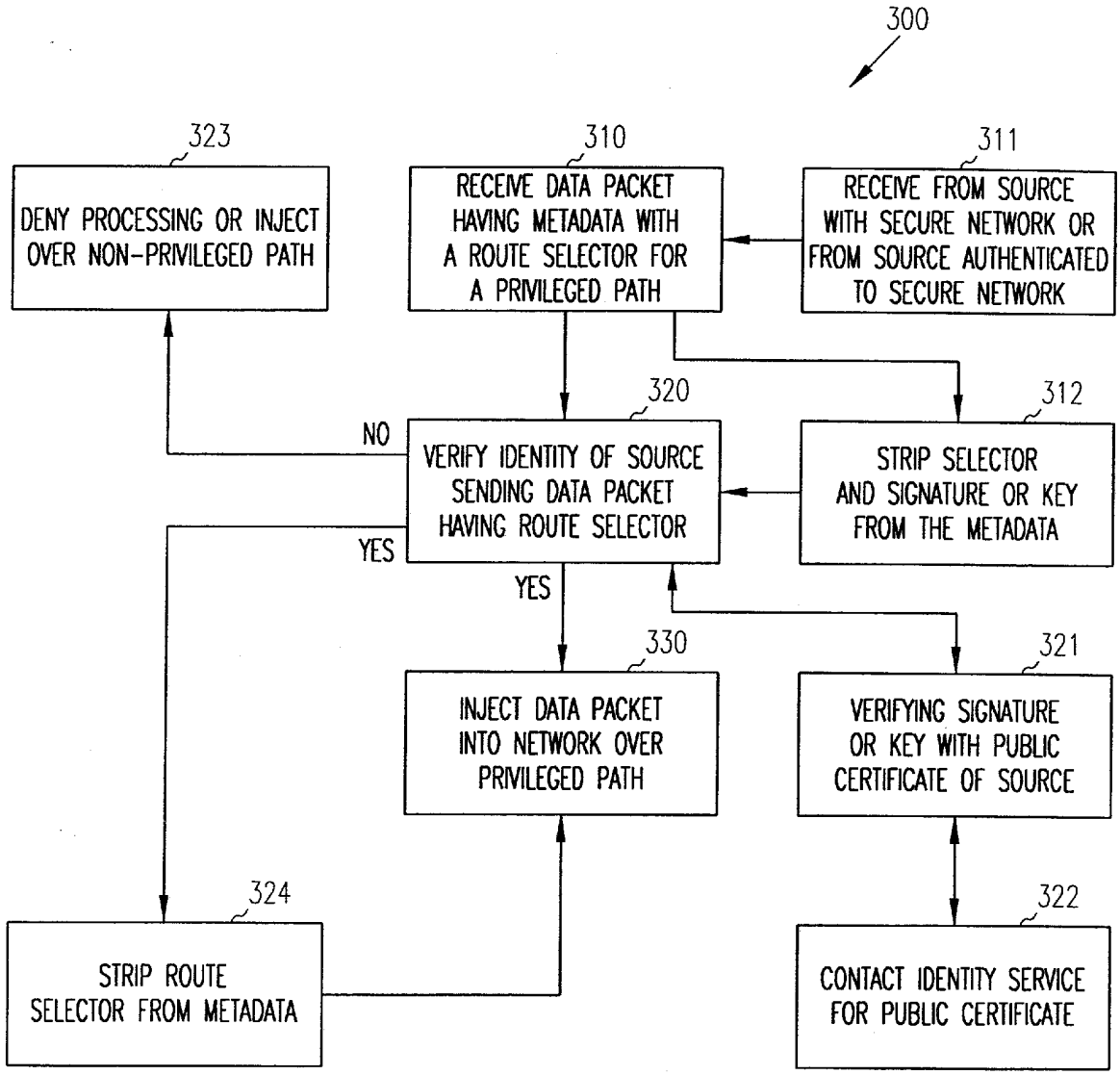
300
323
DENY PROCESSING OR INJECT OVER NON-PRIVILEGED PATH
310
RECEIVE DATA PACKET HAVING METADATA WITH A ROUTE SELECTOR FOR A PRIVILEGED PATH
311
RECEIVE FROM SOURCE WITH SECURE NETWORK OR FROM SOURCE AUTHENTICATED TO SECURE NETWORK
320
NO
VERIFY IDENTITY OF SOURCE SENDING DATA PACKET HAVING ROUTE SELECTOR
312
STRIP SELECTOR AND SIGNATURE OR KEY FROM THE METADATA
YES
YES
330
INJECT DATA PACKET INTO NETWORK OVER PRIVILEGED PATH
321
VERIFYING SIGNATURE OR KEY WITH PUBLIC CERTIFICATE OF SOURCE
324
STRIP ROUTE SELECTOR FROM METADATA
322
CONTACT IDENTITY SERVICE FOR PUBLIC CERTIFICATE

FIG. 3

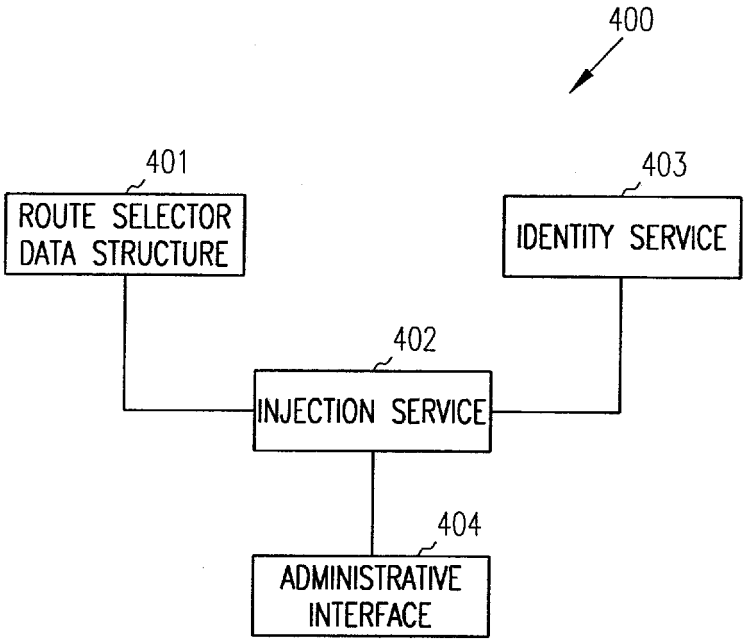
400
401
ROUTE SELECTOR DATA STRUCTURE
403
IDENTITY SERVICE
402
INJECTION SERVICE
404
ADMINISTRATIVE INTERFACE

FIG. 4

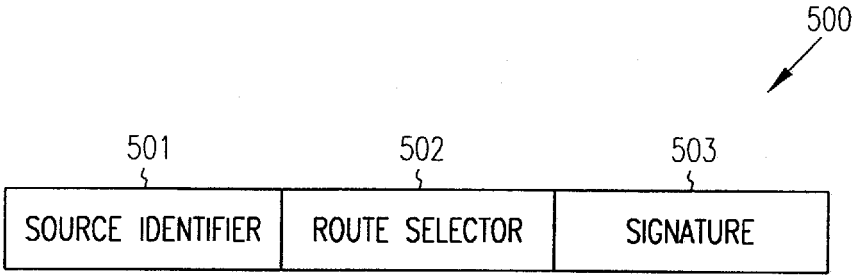
500
501
SOURCE IDENTIFIER
502
ROUTE SELECTOR
503
SIGNATURE

FIG. 5